BY ORDER OF THE SUPERINTENDENT *AFI 31-401*

HQ UNITED STATES AIR FORCE ACADEMY
Supplement 1

12 AUGUST 2001

Security

INFORMATION SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publications is available electronically on the Academy Website (www.usafa.af.mil/scs/afapbf.htm).

OPR: 10 SFS/SFAI (Mrs. Bowen) Certified by: 10 SFS/SFA (MSgt Richard Owens)
Supersedes AFI 31-401/Sup 1, 20 July 1999 Pages: 9
Distribution: F

AFI 31-401, 1 January 1999, was supplemented as follows:

An (*) indicates revisions from the previous edition.

1.3.4. The Commander, 10th Security Forces Squadron (10 SFS/CC), is the Information Security Program Manager (ISPM) at the USAF Academy.

1.3.4.2. Information Security (10 SFS/SFAI) implements and administers the Information, Personnel, and Industrial Security Programs for 10 SFS/SF. All agencies, including tenant units, route correspondence pertaining to issues under these programs through 10 SFS/SF to 10 SFS/SFAI before processing to the Air Staff.

1.3.4.2.1. (Added). 10 SFS/SFAI will provide program oversight by conducting staff assistance visits (SAV) at the request of the unit commander or staff agency chief to determine the level of security education and knowledge by unit or agency personnel. These visits will be assistance oriented and designed to identify unit training strengths and weaknesses. Visits may be conducted more frequently, as determined by 10 SFS/SF, based on discrepancies identified during the semiannual self-assessment, or if requested by unit commanders or agency chiefs. Recurring security problems having a high potential for causing security incidents may also be rationale for conducting more frequent visits.

1.3.4.3. 10 SFS/SFAI personnel will be available for presentations at unit training sessions, commander's calls, and other types of briefings or training sessions upon request. Notify 10 SFS/SFAI immediately upon determining event date to provide sufficient planning time.

1.3.4.3.1. (Added). 10 SFS/SFAI will periodically provide training plans, security education pamphlets, posters, articles, and training aids to assist security managers in meeting recurring security education and training requirements.

1.3.5.1. Notify 10 SFS/SFAI immediately upon change of security managers. Security managers will be trained by either a one-on-one training session or in a group training session scheduled by 10 SFS/SFAI. Training will commence within 30 days of notification to 10 SFS/SFAI. Training will cover the Electronic Personnel Security Questionnaire (EPSQ), and all pertinent forms, information on the Clearance Access Verification System (CAVS), and procedures for the protection of classified information.

1.3.5.1.1. (Added). Primary security managers should be in the grade of staff sergeant or above (or civilian equivalent). Also, appoint at least one alternate security manager (senior airman/GS-4 or above) to perform these duties in the absence of the primary security manager. Commanders or staff agency chiefs appoint security managers by memorandum identifying the appointee's name, rank, office symbol, and duty phone. Send a copy of the appointment memorandum to 10 SFS/SFAI.

*1.3.6.1. Security Managers will organize the Information Security Program and maintain a current roster identifying access of all personnel in the unit.

*1.3.6.2. The Security Manager will keep the unit commander advised on security issues pertaining to the unit.

*1.3.6.3. The Security Manager will update and remind personnel of security policies and procedures on a quarterly basis.

*1.3.6.4. The Security Manager will assist the unit commander and ISPM in monitoring security incident investigations. The unit discovering the incident will make the first report and continue to monitor the incident if they have involved in any capacity.

*1.4.3. Units and activities that do not store, possess, or frequently process classified materials may conduct annual self-assessments.

*1.4.3.1. It is recommended the Security Manager should not conduct self-inspections themselves but have others in the unit perform them.

1.6.1. Send all requests for waivers through 10 SFS/SFAI to 10 SFS/SF.

2.1.2.3. The Superintendent (HQ USAFA/CC) is the designated original classification authority (OCA) for the USAF Academy up to and including SECRET.

2.3.1.1. Include the Information Security Section (10 SFS/SFAI) in the review process for all challenges to classification.

5.6.1. At the USAF Academy, HQ USAFA/CV is the approval authority.

5.10.1.2. No activity will store TOP SECRET material without coordinating with 10 SFS/CC and 10 SFS/SFAI.

*5.12. It is mandatory to check each classified storage container at the end of each duty day, even if the container has not been opened since the previous check. Annotate checks on the SF 702.

5.14.1. The Commander, 10th Air Base Wing (10 ABW/CC), designates overnight repository facilities. The Law Enforcement Desk (10 SFS/SFOL) is designated as the overnight repository for transient classified material up to the SECRET level. Activities hosting classified lectures and visitors who possess classified material at the SECRET level or below are responsible for ensuring the classified material is properly stored within their activity. If the hosting activity does not maintain appropriate storage containers, the host activity is responsible for making storage arrangements with another agency, which has an approved storage container, prior to the arrival of the classified materials. Activities hosting classified events with large quantities of classified material, classified hardware, or classified equipment must coordinate with 10 SFS/SFAI at least 10 duty days prior to the event to ensure availability of storage space.

5.15.2. 10 ABW/CC approves secure conference facilities. The hosting activities for classified briefings should contact 10 SFS/SFAI for guidance. Any area where classified information is discussed must provide adequate security against unauthorized access. This is especially important when classified information may be heard from the exterior of the facility. Establish entry control procedures and perimeter area surveillance by posting appropriately cleared personnel from the sponsoring activity outside of the facility or room. Security Forces is not responsible for this function. The sponsoring activity or OPR of any classified meeting, class, or conference is responsible for complying with the requirements for protecting, safeguarding, and disposing of classified material. Advice may be obtained from 10 SFS/SFAI if the security requirements are beyond the scope of the OPR or the sponsoring activity.

5.19. Prior to purchasing a new security container, coordinate requests with 10 SFS/SFAI.

*5.20.1. USAF Academy activities with small amounts of classified material, up to and including SECRET, may store the material in another unit's storage container if approved by the storing agency. The storing agency must be involved in the USAF Academy's Information Security Program. Identify in the unit's OIs where the materials are stored and identify the office symbol of the point of contact within the storing agency.

5.20.1.1. (Added). The commander or staff agency chief will provide a memorandum to the storing unit identifying the owning agency's office symbol, date of last review, and a list of personnel authorized access to the classified material.

5.20.2. 10 ABW/CC determines what areas are permitted to be used as open or unattended storage areas and approves storage of classified material in these areas.

5.20.2.1. (Added). Classified material must be wrapped, sealed with nylon reinforced paper tape, and marked with the highest overall classification. A memorandum containing the owning agency's office symbol, the date of the last review, and a list of personnel authorized access to the classified material will be physically attached to the outside of the wrapped material. A sample memorandum is shown at Attachment 7 (Added-USAFA) for the recommended format.

5.25. (USAFA). Post AFTO Form 36 inside the locking drawer of the container and annotate each time maintenance is performed.

5.26.1. (USAFA). Commanders must designate, in writing, specific equipment to be used for reproduction (copiers) of classified material, after approval with the Defense Automated Printing Service (DAPS) and coordination with 10 SFS/SFAI. DAPS will control the equipment used for reproduction of classified material by HQ USAFA units and activities. Refer to DODD 5330.3/Air Force Supplement, *Defense Automated Printing Service (DAPS).*

*5.26.3.1 Unit Security Managers will post correct documents to identify equipment approved for copying classified material.

*5.26.3.2. Unit Security Managers will ensure personnel understand the security responsibilities and follow all procedures.

*5.28.3. When the self-inspection is performed, 6 months after the annual program review, the unit security manager must coordinate with the owning agency for an inspection and determine whether the material is still required for operational purposes or can be destroyed.

*5.28.3.1. (Added). Periodically review and destroy classified materials throughout the year as needed. Unit security managers should establish the frequency for classified review and destruction in the unit or agency security OIs.

5.29.1. There is no central classified destruction facility at the Academy. Each unit or agency that destroys classified material must either purchase a shredder which meets the specifications of DoD 5200.1-R for destroying classified material or arrange to use another agency's shredder which meets these specifications. Prior to purchasing any shredder, coordinate with 10 SFS/SFAI to ensure the appropriate type shredder is being purchased. Contact 10 SFS/SFAI for guidance on what equipment or facilities are available for destruction of large quantities of classified material.

5.29.2. The owning agency remains responsible for all declassification actions and must establish and maintain destruction certificates for SECRET and TOP SECRET material.

5.29.2.1.1. HQ USAFA/CV is the waiver authority for the two-person policy.

6.1.1. **Do not use USAFANET to send classified messages or letters to anyone.** Do not use any computer system to process classified information unless specifically approved, in writing, by Base Information Protection (10 CS/SCXS). Send all classified electronically transmitted messages through the base telecommunications center. All classified material to be dispatched off the Academy must be properly wrapped with an AF Form 12, **Accountable Container Receipt**, attached. Forward the package through the Base Information Transfer Center (BITC) for dispatch by the U.S. Postal Service.

7.1.1. 10 SFS/SFAI is the certification authority on the Department of Energy (DOE) Form 5631.20 for USAF Academy units and agencies.

8.9. Security managers prepare and submit a copy of the unit's annual training plan to 10 SFS/SFAI and file the original in the unit security manager's handbook. The annual training plan should identify what topic will be presented each calendar quarter and how the training will be conducted (video, briefing, etc.).

9.2.1. Unit commanders, of the unit causing the incident, are responsible for briefing the appropriate wing commander on all-open inquiries and formal investigations pertaining to security incidents. All staff agencies report open inquiries and investigations of this type to the appropriate staff agency chief. Wing commanders and staff agency chiefs must ensure that HQ USAFA/CV is briefed on the findings and final disposition of all preliminary inquiries and formal investigations related to security incidents occurring at the USAF Academy.

9.2.4. Notify AFOSI Detachment 808 at the USAF Academy for these violations.

9.3.2.1. Unit commander and staff agency chiefs should first consider appointing personnel who are not charged with information security program implementation responsibilities such as the unit security manager or alternate. Refer to DoD 5200.1-R, chapter 10; and AFI 31-401, chapter 6, for guidance on conducting these inquiries. Contact 10 SFS/SFAI for additional assistance as needed.

9.3.2.2. If damage to national security is determined, the 10 ABW/CC will appoint a formal investigation official. 10 ABW/CC may appoint investigation officials through the base detail program. If the incident occurs during nonduty hours, notify 10 SFS/SFAI no later than the next duty day. 10 SFS and the Inspector General (HQ USAFA/IG) will not be tasked to serve in an official investigation. Investigation officials are encouraged to contact 10 SFS/SFAI for additional guidance as required.

9.3.2.3. Appointed officials should coordinate with 10 SFS/SFAI prior to closing all preliminary inquiries to ensure no further action is required. Send copies of all inquiries and investigations

through 10 SFS/SFAI to 10 SFS/SF for review upon completion. Disagreements between the unit commander and 10 SFS/SF on how an inquiry is closed will be forwarded to the appropriate wing commander for a decision. Disagreements between staff agency chiefs or wing commanders and 10 SFS/SF will be forwarded to HQ USAFA/CV for a final decision on closure of the inquiry.

9.4.1.2. When someone is determined to be responsible for the security incident, coordinate with the appropriate Staff Judge Advocate's office to determine if administrative or disciplinary action is appropriate. 10 ABW/CC is the final approval authority for all formal investigations conducted at the USAF Academy. Forward all investigation reports through 10 SFS/SF and the Staff Judge Advocate (10 ABW/JA) for review before sending to 10 ABW/CC.

9.4.1.4. Close and forward inquiry reports to the appointing official within 30 days from the date of appointment. The appointing official may approve extensions of the suspense date. 10 SFS/SFAI receives copies of closed inquiry reports and formal investigations on security incidents.

9.5.1. Upon notification of a possible compromise or compromise of any materials originally classified by HQ USAFA/CC, functional OPRs of the information will immediately notify 10 SFS/SFAI. Be prepared to identify the documents involved along with the details of where, when, and how the compromise occurred. Also, include a point of contact and DSN number at the unit or installation where the compromise occurred. Functional OPRs of classified material will conduct an immediate review of the information, which was or may have been compromised and determine the extent of damage possible and possible consequences of the compromise. Route this information through 10 SFS/SF to HQ USAFA/CC. Other coordination requirements will be determined by 10 SFS/SF based upon the OPR of the materials involved and the level of notification required outside of HQ USAFA.

9.8. (Added). Forms Adopted. AF Form 12, **Accountable Container Receipt.**

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

Abbreviations and Acronyms

CAVS—Clearance Access Verification System

EPSQ—Electronic Personnel Security Questionnaire

Attachment 3

Controlled Unclassified Information

A3.4.2.1.4. 10 SFS/SF is the authorized official to identify and deny release of DoD Unclassified Controlled Nuclear Information (UCNI) at the USAF Academy.

ATTACHMENT 7 (Added)

SAMPLE MEMORANDUM

(USE APPROPRIATE ORGANIZATIONAL LETTERHEAD)

MEMORANDUM FOR UNIT (UNIT CONTROLLING THE SAFE)

FROM: Unit (Owning Agency)

SUBJECT: Personnel Authorized Access to Attached Classified Material

1. The following information is provided in reference to the attached classified material:

   a. Owning agency's office symbol.

   b. Date of last review.

   c. List of personnel authorized access to the classified material.

2. Direct questions to the unit security manager, MSgt Doe, at 3-xxxx.

UNIT COMMANDER
Title Designation

WILLIAM D. SELLERS, Lt Col, USAF

Chief, Security Forces